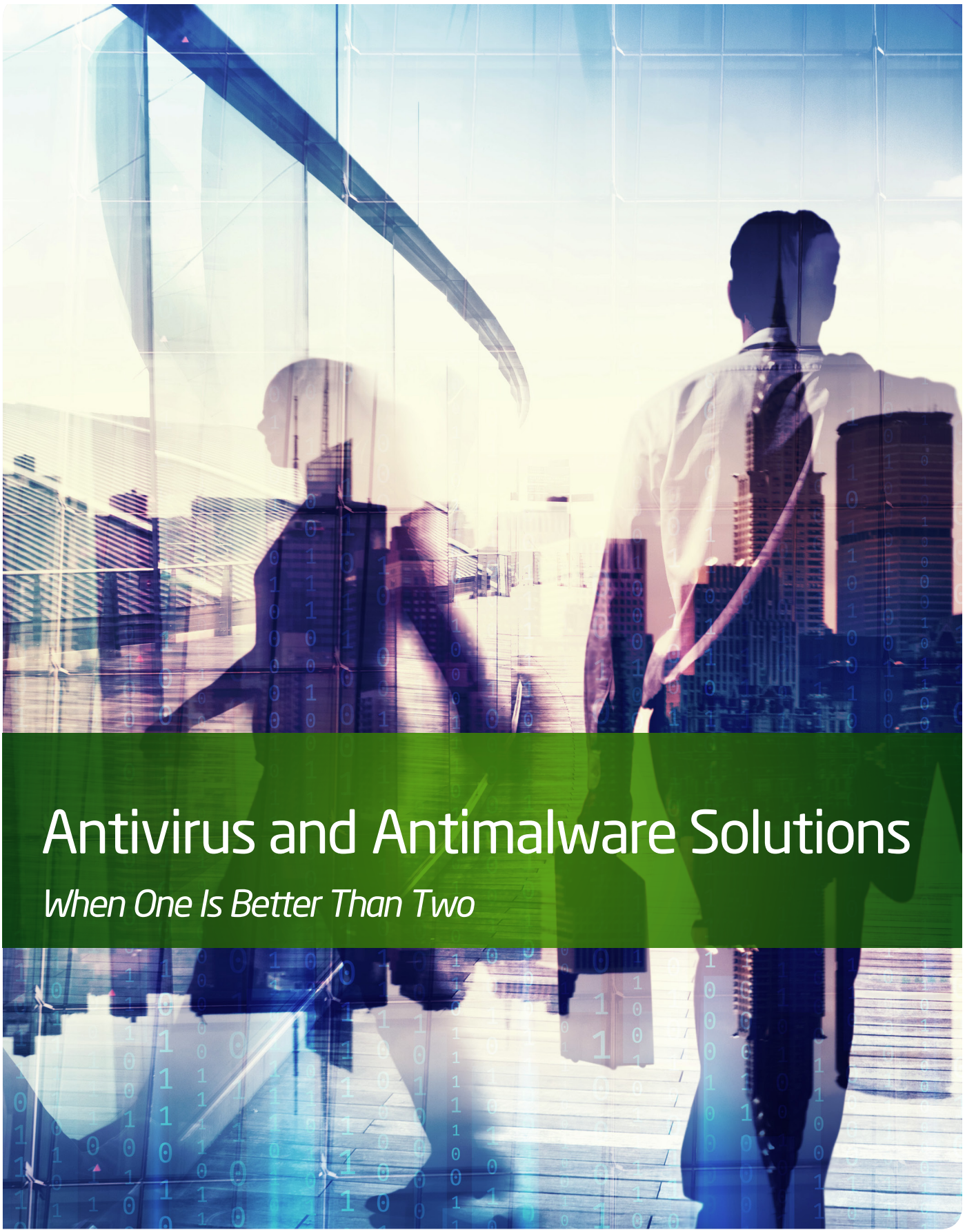
WEBROOT®



Antivirus and Antimalware Solutions

When One Is Better Than Two

APRIL 2015

TABLE OF CONTENTS

BACKGROUND

Perhaps more than any other type of software solution a reseller can offer to its customers, endpoint security products are characterized by a huge gap between their minimal purchase prices and the enormous costs they can entail for clients if they fail to work properly. The financial benefits of retailing antivirus solutions are modest (typical street prices are $24/year per seat, with VAR cost roughly $12), while the potential losses suffered by a VAR's customer due to virus or malware infections can be devastating.

Such costs can range from system downtime and diminished productivity to lost sales revenues and even potential legal liability for claims relating to any private information that may have been compromised. Combating the alarming volume, velocity and variance of today's security threats has become significantly more challenging as cybercriminals employ an extensive range of sophisticated new techniques (polymorphism, spear phishing, etc).

Yet, despite this rapidly-evolving threat landscape—and the substantial financial hardships it can impose on resellers' customers—many VARs still underestimate the importance of offering the optimum antivirus solution. By focusing on the modest acquisition expenses of antivirus products, VARs may tend to overlook the significant business consequences and huge costs for its customers that choosing the wrong endpoint security solution can entail.

"What's more, the damage from virus and malware infections also affects VARs. Customer dissatisfaction and frustration arising from such incidents undermines trust in the VAR and with it the likelihood of long-term patronage (and thus its recurring, predictable revenue). It also jeopardizes a VAR's ability to cultivate a trusted advisor relationship with its customers that can open up a multitude of other business opportunities."

DRAWBACKS OF MULTI-SOLUTION ANTIVIRUS STRATEGIES

In an effort to deliver more comprehensive protection to their customers, some VARs have resorted to recommending a combination of two separate and distinct antivirus products. The motivation for this approach often stems from the presence of new threats that many well-established antivirus solutions are unable to address.

For example, CryptoLocker is a new and highly disruptive security threat, belonging to a family of malware called "ransomware." It's designed to extort money from victims by denying them access to their personal files. Because of the complex encryption strategy it utilizes, such malware is nearly impossible to remediate once it has infected a customer's computers. The best protection against such infections requires a preventive approach.

Unfortunately, VARs have found that a substantial number of high-profile antivirus solutions are ineffective in preventing such infections, and thus have been forced to add a second solution to their customer recommendations.

"This approach entails several downsides, but higher antivirus solution purchase costs for the VAR's customer is not among them. That expense is still relatively trivial. Instead, it is the increased cost in time imposed by multiple antivirus solutions that can frustrate and alienate customers. The man-hours needed to deploy and manage a typical signature-based antivirus can be substantial, and they become even more onerous when customers must use two separate products to ensure complete protection from the latest malware threats such as CryptoLocker."

Whenever an antivirus vendor releases signature updates, a VAR's customer must download those updates and schedule when they can be pushed out from its dedicated server to every desktop and endpoint device in the customer's IT environment. Best practices dictate testing any updates first, but using two antivirus solutions requires evaluating two sets of updates. A customer's IT staff may be tempted to simply push out both sets of untested signatures, which can result in crashed systems and significantly diminished customer productivity.

Further productivity losses can also be traced to the use of multiple antivirus solutions. Traditional antivirus client software compares every file on the user's computer against the myriad definitions in the signature database within the client. These scans consume a huge amount of processing power, so much so that during scans an end user's computer is essentially rendered useless. These signature-based slowdowns are a leading source of customer discontent, and they become far more disruptive and extensive when imposed by two separate antivirus solutions.

Additional drawbacks to the multiple-solution antivirus approach include the need for customers to learn the different user interfaces and management dashboards for each of the separate antivirus solutions. This can make management far more time-consuming for the customer's IT staff. And, the simultaneous use of multiple antivirus solutions introduces the potential for operational conflict, a particularly challenging problem as antivirus solutions are not typically designed for concurrent duty with another endpoint security product.

WHY A SINGLE ANTIVIRUS SOLUTION IS BETTER

Webroot has applied modern technologies and methodologies to its endpoint security solutions, resulting in single antivirus offerings that deliver fundamentally superior protection, ease of use and performance to customers compared with any combination of conventional antivirus products. As a result, resellers can provide greater security and peace of mind to their customers with just one antivirus solution. In so doing, VARs will not only help their clients save money and simplify the purchase, deployment and management of antivirus protection, they'll also significantly strengthen their business relationships with those customers.

The most obvious characteristic differentiating Webroot endpoint security solutions from competitors is their completely cloud-based architecture. This enables the use of a lightweight client (under 1 MB), because no signature database is stored within the client software. Instead Webroot maintains a massive signature database in the cloud. This approach combines far better protection, quicker installation and faster scanning. Average scans complete in a matter of seconds, reducing your customer's IT overhead while improving its productivity and uptime.

Webroot® security solutions also use cloud-predictive behavioral intelligence to discover malware as soon as it attempts to infect your customer. And, because Webroot endpoints collect over 200 gigabytes of behavioral execution data each day, Webroot solutions become more powerful every minute, strengthening their ability to automatically detect a CryptoLocker infection variant before it can infect and make changes to the computer.

CONCLUSION

Cobbling together multiple antivirus products to ensure their customers have adequate endpoint security is clearly not a strategy most VARs favor. It is a costly, complex kludge that attempts to compensate for the inherent deficiencies of conventional signature-based antivirus solutions. But, there is a better way.

Simply put, Webroot maximizes your customers' security, cuts bandwidth utilization, reduces resource loads on PCs, and shrinks antivirus disk space use. All the while, its web-based centralized console streamlines management, saving your clients time—and money—on administration of their endpoint devices. Equally important, it cements your status as a trusted advisor to your customers by demonstrating an ability to deliver the best solutions available.

About Webroot

Designed with MSPs, resellers, distributors and other providers in mind, the Webroot® Channel Edge® Program offers competitive margins, recurring revenue, lower operational costs, improved productivity, and innovative enablement tools. Through its web-based management console or integration with RMM and PSA platforms, Webroot offers smart, easy-to-deploy protection for endpoint, mobile and web. Partnering with businesses of all sizes, Webroot secures your workforce against sophisticated threats—no matter how or where users connect.

We offer local support by real Webroot employees around the world, in your time zone, and in over 60 languages. Webroot cares about total customer satisfaction, and we're never more than a click away.

For more information, visit www.webroot.com/us/en/partners

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
800 772 9383

Webroot EMEA
6th floor, Block A,
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0)870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900